


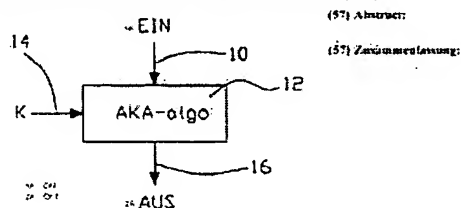


**AUTHENTICATION SYSTEM AND METHOD BETWEEN TWO COMMUNICATIONS UNITS****Publication number:** WO03056863 (A2)**Publication date:** 2003-07-10**Inventor(s):** TIETZ BENNO [DE]; RUEDINGER JENS [DE]; BABBAGE STEPHEN [GB]**Applicant(s):** VODAFONE HOLDING GMBH [DE]; TIETZ BENNO [DE]; RUEDINGER JENS [DE]; BABBAGE STEPHEN [GB]**Classification:****- International:** H04W12/00; H04W12/00; (IPC1-7): H04Q7/38**- European:** H04W12/06; H04Q7/38S**Application number:** WO2002EP14411 20021217**Priority number(s):** DE20021000041 20020103**Also published as:** EP1470733 (A2) AU2002361000 (A1) DE10200041 (A1)Abstract not available for **WO 03056863 (A2)**

Data supplied from the esp@cenet database — Worldwide

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES  
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
10. Juli 2003 (10.07.2003)

PCT

(10) Internationale Veröffentlichungsnummer  
**WO 03/056863 A2**

(51) Internationale Patentklassifikation<sup>7</sup>: H04Q 7/38

SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG,  
US, UZ, VN, YU, ZA, ZM, ZW.

(21) Internationales Aktenzeichen: PCT/EP02/14411

(22) Internationales Anmeldedatum:  
17. Dezember 2002 (17.12.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:  
102 00 041.7 3. Januar 2002 (03.01.2002) DE

(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von  
US): VODAFONE HOLDING GMBH [DE/DE]; Man-  
nesmannufer 3, 40213 Düsseldorf (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): TIETZ, Benno  
[DE/DE]; An der Wasserburg 17 h, 51067 Köln (DE).  
RÜDINGER, Jens [DE/DE]; Wülfrather Str. 3, 40233  
Düsseldorf (DE). BABBAGE, Stephen [GB/GB]; 92  
Andover Road, Newbury RG14 6JR (GB).

(74) Anwälte: WEISSE, Jürgen usw.; Bökenbuschstr. 41,  
42555 Velbert (DE).

(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT,  
AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,  
CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE,  
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR,  
KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK,  
MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU,

(84) Bestimmungsstaaten (regional): ARIPO-Patent (GH,  
GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),  
eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ,  
TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE,  
DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT,  
SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM,  
GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Erklärungen gemäß Regel 4.17:

— hinsichtlich der Identität des Erfinders (Regel 4.17 Ziffer  
i) für die folgenden Bestimmungsstaaten AE, AG, AL, AM,  
AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR,  
CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE,  
GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ,  
LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW,  
MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,  
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA,  
ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD,  
SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY,  
KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE,  
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT,  
LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF,  
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

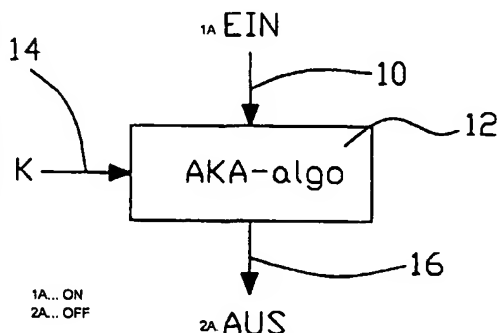
— hinsichtlich der Berechtigung des Anmelders, ein Patent zu  
beantragen und zu erhalten (Regel 4.17 Ziffer ii) für die  
folgenden Bestimmungsstaaten AE, AG, AL, AM, AT, AU,  
AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,  
CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH,  
GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC,  
LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,  
MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK,

[Fortsetzung auf der nächsten Seite]

(54) Title: AUTHENTICATION SYSTEM AND METHOD BETWEEN TWO COMMUNICATIONS UNITS

(54) Bezeichnung: AUTHENTIFIZIERUNGSSYSTEM UND -VERFAHREN ZWISCHEN ZWEI KOMMUNIKATIONSEIN-  
HEITEN

WO 03/056863 A2



(57) Abstract:

(57) Zusammenfassung:



SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW, ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

**Veröffentlicht:**

— mit einer Erklärung gemäss Artikel 17 Absatz 2 Buchstabe a; ohne Zusammenfassung; Bezeichnung von der Internationalen Recherchenbehörde nicht überprüft

Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

**Authentifizierungssystem und -verfahren zwischen zwei Kommunikationseinheiten****Technisches Gebiet**

Die Erfindung betrifft ein Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten, wobei zwischen den Kommunikationseinheiten eine Authentifizierungsvereinbarung besteht, welche jeweils durch eine prozessorgestützte Authentifizierungseinheit überprüft werden kann, wobei die Authentifizierungsvereinbarung aus wenigstens zwei unterschiedlichen Authentifizierungsalgorithmen besteht, welche in einer Speichereinheit wenigstens einer der Kommunikationseinheiten vorgesehen sind und welche durch die jeweilige andere Kommunikationseinheit zur Authentifizierung abgefragt werden kann. Ferner betrifft die Erfindung ein Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten, wobei zwischen den Kommunikationseinheiten eine Authentifizierungsvereinbarung besteht, welche jeweils durch eine prozessorgestützte Authentifizierungseinheit überprüft werden kann, wobei die Authentifizierungsvereinbarung aus wenigstens zwei unterschiedlichen Authentifizierungsalgorithmen besteht, welche in einer Speichereinheit wenigstens einer der Kommunikationseinheiten vorgesehen sind und welche durch die jeweilige andere Kommunikationseinheit zur Authentifizierung abgefragt werden kann.

## Stand der Technik

Bei Kommunikationseinheiten, wie z.B. Mobilfunktelefone und Mobilfunknetz, wird die Berechtigung für einen Netzwerkteilnehmer durch das Kommunikationsnetz abgefragt. Der Schutz gegen unberechtigten Zugang zum Kommunikationsnetz sowie Mißbrauch ist ein unverzichtbares Merkmal moderner Kommunikationsnetze, wie es beispielsweise das GSM- und das UMTS-Netz darstellen. Bei diesen Netzwerken gilt es, insbesondere die offene Funkschnittstelle zu schützen.

Um den Netzbetreiber vor solchen unberechtigten Nutzungen des Netzes und den Teilnehmer vor Mißbrauch seiner Zugangsberechtigung zu schützen, ist eine sichere Teilnehmeridentifikation bei Kommunikationswünschen erforderlich. Die Häufigkeit der Überprüfung dieser Identifikation wird in der Regel durch den Netzbetreiber festgelegt. Eine mögliche Authentifikation eines Netzwerkteilnehmers ist insbesondere im GSM-Standard definiert. Sie erfolgt nach einem Aufforderungs-Antwortverfahren (Challenge/Response) zwischen der authentisierenden Stelle des Kommunikationsnetzes und der Kommunikationseinheit. Dazu wird von der authentisierenden Stelle – auch Authentifikationszentrum (AuC) genannt – des Kommunikationsnetzes eine Zufallszahl "RAND" generiert, die der Kommunikationseinheit übermittelt wird. Die Kommunikationseinheit berechnet aus der Zufallszahl "RAND" unter Benutzung eines Teilnehmerschlüssel bzw. Authentifizierungsschlüssel " $K_i$ " und eines Authentifikationsalgorithmus "A3" die Prüfsumme "SRES" und sendet diese an die authentisierende Stelle zurück. In der authentisierenden Stelle werden nun die von der Kommunikationseinheit zurückgesendete Prüfsumme "SRES" mit der von ihr selbst analog berechneten Prüfsumme "XSRES" verglichen. Stimmen beide Prüfsummen "SRES" und "XSRES" überein, so ist die Authentifikation erfolgreich bestanden.

Gleichzeitig mit der Durchführung der Authentifikation wird unter Benutzung des Teilnehmerschlüssels  $K_i$  und des Datenschlüsselgenerierungsalgorithmus "A8" aus der Zufallszahl "RAND" in der Kommunikationseinheit und in dem Kommunikationsnetz ein neuer Teilnehmerschlüssel  $K_c$  berechnet. Das Kommunikationsnetz vergibt

zusammen mit der Zufallszahl "RAND" die dazugehörige Schlüsselnummer CKSN, die zusammen mit  $K_c$  in der Kommunikationseinheit und in dem Kommunikationsnetz gespeichert wird.

Die WO 99/62275 beschreibt ein Verfahren zur Steuerung eines Teilnehmeridentitätsmoduls (SIM) in Mobilfunksystemen, bei denen daß Mobilfunknetz einen oder mehrere bestimmte Steuerwerte an das Teilnehmeridentitätsmodul sendet, die bestimmte Aktionen innerhalb des Teilnehmeridentitätsmoduls auslösen. Dabei werden als Steuerwerte bestimmte und vom Mobilfunknetz für die reguläre Authentifikation an das Teilnehmermodul gesendete Zufallswerte verwendet. Dort wird beschrieben, daß zur Erhöhung der Sicherheit im Mobilfunknetz bei diesem Verfahren z.B. auf der SIM mehrere verschiedene Sicherheitsalgorithmen abgelegt sein können, zwischen welchen durch Empfang eines entsprechenden Steuerwertes umgeschaltet werden kann. Ebenso ist möglich, daß auf der SIM-Karte mehrere geheime Schlüssel  $K_i$  abgelegt sind, oder aus einem dort abgelegten Schlüssel hergeleitet werden können, zwischen welchen durch Empfang eines entsprechenden Steuerwertes umgeschaltet werden kann. Ferner besitzt die SIM-Karte zwei verschiedene, oder auch mehrere Algorithmen, die die gleichen Schnittstellen nach außen besitzen, bei gleicher Länge von RAND,  $K_i$  und SRES. Dabei kann die SIM nur einen  $K_i$ , oder je Algorithmus einen eigenen  $K_i$  besitzen. Möchte der Netzbetreiber aus Sicherheitsgründen den verwendeten Algorithmus A3/A8 wechseln, kann er das Authentifikationszentrum AuC veranlassen, eine spezielle Zufallszahl RAND zu erzeugen, welche gleichzeitig einen erfindungsgemäßen Steuerwert darstellt, der auch als Steuer-RAND bezeichnet wird.

Nachteile der genannten Authentifizierungssysteme ergeben sich dadurch, daß die Authentifizierungsvorgänge im wesentlichen sequentiell bei der Verarbeitung ablaufen. Hierdurch kann es zu Verzögerungen bei der Authentifizierung kommen.

## Offenbarung der Erfindung

Aufgabe der Erfindung ist es daher, ein Authentifizierungssystem und ein entsprechendes Verfahren zu Authentifizierung für zumindest zwei Kommunikationseinheiten zu schaffen, bei dem die Nachteile des Standes der Technik beseitigt werden. Ferner ist es Aufgabe der Erfindung, kostengünstig die Sicherheit zu erhöhen, ohne erheblichen technischen Mehraufwand betreiben zu müssen.

Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß bei einem Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten der eingangs genannten Art, Mittel zur gleichzeitigen dynamischen Verarbeitung der Authentifizierungsalgorithmen vorgesehen sind. Ferner wird die Aufgabe durch ein Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten der eingangs genannten Art gelöst, bei dem die Authentifizierungsalgorithmen gleichzeitig dynamisch abgearbeitet werden.

Das Prinzip eines erfindungsgemäßen Authentifizierungssystems besteht insbesondere darin, daß neben den Identifikationsdaten und der Adresse desjenigen Teilnehmers, der sich authentifizieren muß, gleichzeitig die Rückadresse übermittelt wird. Hierdurch kann eine gleichzeitige Abarbeitung der Authentifizierung sowohl durch die eine Kommunikationseinheit, als auch durch die entsprechende andere Kommunikationseinheit vorgenommen werden. Die Berechnung der Prüfsummen erfolgt daher nunmehr von beiden Kommunikationseinheiten parallel, im Sinne von gleichzeitig. Durch den Wechsel zwischen verschiedenen Authentifizierungsalgorithmen die quasi gleichzeitig zwischen den Kommunikationseinheiten erfolgt, erhält man ein höheres Maß an Sicherheit. Nicht nur in Mobilfunknetzen kann es erforderlich sein, eine Authentifizierung eines Kommunikationsteilnehmers vorzunehmen, sondern auch in Festnetzen. Bei Kommunikationsnetzen spielt die Sicherheit eine immer größere Rolle, um die Netzbetreiber vor unberechtigten Nutzungen des Netzes und den Teilnehmer vor Mißbrauch seiner Zugangsberechtigung zu schützen.

Auch das Prinzip des erfindungsgemäßen Verfahrens zum Authentifizieren zweier Kommunikationseinheiten besteht darin, neben den Identifikationsdaten und der Adresse desjenigen Teilnehmers, der sich authentifizieren muß, gleichzeitig die Rückadresse zu übermitteln. Hierdurch kann eine gleichzeitige Abarbeitung der Authentifizierung sowohl durch die eine Kommunikationseinheit, als auch durch die entsprechende andere Kommunikationseinheit vorgenommen werden. Die Berechnung der Prüfsummen erfolgt daher nunmehr von beiden Kommunikationseinheiten parallel, im Sinne von gleichzeitig. Durch den Wechsel zwischen verschiedenen Authentifizierungsalgorithmen, die quasi gleichzeitig zwischen den Kommunikationseinheiten erfolgt, erhält man ein höheres Maß an Sicherheit.

In einer vorteilhaften Ausgestaltung des erfindungsgemäßen Authentifizierungssystems ist die eine Kommunikationseinheit als Mobilfunkendgerät ausgebildet. Gerade bei einem Mobilfunkendgerät besteht ein hoher Authentifizierungsbedarf. Über die relativ anfällige Luftschnittstelle kann sich ein Dritter leicht zwischen zwei Kommunikationseinheiten schalten und Mißbrauch betreiben. Bei der Benutzung zweier Mobilfunkendgeräten kann es beispielsweise erforderlich sein, eine möglichst sichere Sprach- bzw. Datentübermittlung zu gewährleisten. Um sicher zu stellen, daß immer der richtige Partner die jeweils andere Kommunikationseinheit verwendet, ist es für die Sicherheit daher vorteilhaft, wenn eine Authentifizierung zwischen beiden Kommunikationseinheiten erfolgt.

In einer Weiterbildung des Authentifizierungssystems sind die Authentifizierungsalgorithmen auf einem Teilnehmeridentitätsmodul ((U)SIM) gespeichert. Da die Teilnehmeridentitätsmodule ((U)SIM) ohnehin personenbezogene Daten enthalten, erscheint es besonders vorteilhaft, die Authentifizierungsalgorithmen auf diesen zu speichern. Von hier aus lassen sich die Authentifizierungsalgorithmen praktisch jederzeit von einer Kommunikationseinheit abrufen. Das Teilnehmeridentitätsmodul ((U)SIM) kann auch geräteunabhängig verwendet werden, d.h. sie kann beispielsweise auch in verschiedenen Mobilfunkendgeräten eingesetzt werden. (U)SIM-Karten sind individuell ausgelegt. Sie lassen sich daher immer einem



bestimmten Teilnehmer zuordnen. Durch diesen Umstand sind SIM-Karten besonders für das Authentifizierungssystem geeignet. Die Authentifizierungsalgorithmen werden auf den individuellen (U)SIM-Karten abgespeichert.

In einer weiteren vorteilhaften Ausgestaltung des erfindungsgemäßen Authentifizierungssystems ist eine Kommunikationseinheit als Authentifikationszentrale eines Kommunikationsnetzes vorgesehen. Durch diese Maßnahme kann der Aufwand der Authentifizierung von Kommunikationsnetzteilnehmern zentral vorgenommen werden. Eine zentralisierte Authentifizierung erlaubt es, schnell auf Änderungen reagieren zu können, um ggf. den Sicherheitsstandard noch weiter zu erhöhen.

In einer Weiterbildung der Erfindung ist wenigstens ein Authentifizierungsschlüssel für die Authentifizierungsalgorithmen vorgesehen. Der Authentifizierungsschlüssel ist ein weiteres Sicherheitsmerkmal für ein erfindungsgemäßes Authentifizierungssystem. Die Kommunikationseinheit berechnet unter Benutzung des Authentifizierungsschlüssel und der Authentifikationsalgorithmen die Prüfsumme. Diese Prüfsumme wird an die Authentifikationszentrale des Kommunikationsnetzes gesendet. In der Authentifikationszentrale wird nun die von der Kommunikationseinheit zurückgesendete Prüfsumme mit der von der Authentifikationszentrale selbst entsprechend berechneten Prüfsumme verglichen. Stimmen beide Prüfsummen überein, so ist die Authentifikation erfolgreich bestanden. Zur Vergrößerung der Sicherheit kann jedem einzelnen Authentifizierungsalgorithmus ein eigener Authentifizierungsschlüssel zugeordnet sein.

In Ausgestaltung des entsprechenden erfindungsgemäßen Verfahrens erweist sich ebenfalls als vorteilhaft, wenn wenigstens eine Kommunikationseinheit als Mobilfunkendgerät ausgebildet ist. In einer besonderen Weiterbildung des Verfahrens werden die Authentifizierungsalgorithmen auf einem Teilnehmeridentitätsmodul ((U)SIM) abgespeichert. (U)SIM-Karten sind individuell ausgelegt. Sie lassen sich daher immer einem bestimmten Teilnehmer zuordnen. Durch diesen Umstand sind (U)SIM-Karten besonders für das Authentifizierungsverfahren geeignet. Die Authentifizierungsalgorithmen werden auf den individuellen (U)SIM-Karten abgespeichert.

In einer besonderen Weiterbildung des Verfahrens ist eine Kommunikationseinheit als Authentifikationszentrale eines Mobilfunknetzes (UMTS/GSM) ausgebildet. Hierdurch lassen sich Authentifizierungsprozesse zentral steuern. Durch Verwendung wenigstens eines Authentifizierungsschlüssels für die Authentifizierungsalgorithmen erhält das erfindungsgemäße Verfahren zur Authentifizierung eine zusätzliche Sicherheitskomponente. Die Sicherheit kann dahingehend noch erhöht werden, indem jedem einzelnen Authentifizierungsalgorithmus je ein eigener Authentifizierungsschlüssel zugeordnet wird.

Weitere Vorteile ergeben sich aus dem Gegenstand der Unteransprüche.

#### **Kurze Beschreibung der Zeichnung**

Fig. 1 zeigt in einer Prinzipskizze die Authentifizierung herkömmlicher Art.

Fig. 2 zeigt eine Prinzipskizze zur Authentifizierung unter Auswahl eines Authentifizierungsalgorithmus.

Fig. 3 zeigt eine Prinzipskizze zur Erzeugung von Teilnehmerschlüsseln.

#### **Bevorzugtes Ausführungsbeispiel**

In Fig. 1 wird eine Prinzipskizze der derzeit verwendeten Authentifizierung für eine Kommunikationseinheit, wie beispielsweise für ein Mobilfunkendgerät mit einem Mobilfunknetz, dargestellt. Mit 10 wird ein Eingang (EIN) bezeichnet. Über den Eingang 10 wird eine Zufallszahl (RAND) an einen Authentifizierungsalgorithmus 12 (AKA-algo) auf Anforderung hin von einer Authentifizierungszentrale (AuC) des Mobilfunknetzes übermittelt. Die Zufallszahl (RAND) wird von der Authentifizierungszentrale (AuC) erzeugt. Der Authentifizierungsalgorithmus 12 ist auf

einem Teilnehmeridentitätsmodul (SIM) gespeichert. Eine Prozessoreinheit arbeitet diesen Authentifizierungsalgorithmus 12 ab. Ein Teilnehmerschlüssel (K) wird über einen weiteren Zugang 14 dem Authentifizierungsalgorithmus 12 zugeführt. Der Teilnehmerschlüssel ermöglicht es, erst den Authentifizierungsalgorithmus 12 ablaufen zu lassen und aus der Zufallszahl (RAND) eine Prüfsumme (SRES) zu bilden. Die Prüfsumme (SRES) wird über Ausgang 16 an die Authentifizierungszentrale (AuC) zurückübertragen. Die Authentifizierungszentrale (AuC) berechnet nun unter gleichen Bedingungen, wie das Mobilfunkendgerät, ebenfalls die Prüfsumme. Stimmen die Ergebnisse überein, so war die Authentifizierungsprozedur erfolgreich.

Im Gegensatz dazu, verfügt das erfindungsgemäße Authentifizierungssystem, wie es in Fig. 2 schematisch dargestellt ist, über wenigstens zwei Eingänge 18, 20. Über Eingang 18 (EIN) wird die Zufallszahl (RAND) dem Authentifizierungssystem zugeführt. Ein Kontrollparameter wird auf den Eingang 20 (Kontrolle) gegeben. Ein Schalter 22 wird durch die Zufallszahl (RAND) und den Kontrollparameter gesteuert. Der Schalter 22 (S) wählt einen der Authentifizierungsalgorithmen 24, 26, 28 aus. Die Auswahl der Authentifizierungsalgorithmen 24, 26, 28 erfolgt zufällig, je nachdem, welche Zufallszahl (RAND) dem Schalter 22 zugeführt wurde. Die Authentifizierungsalgorithmen 24, 26, 28 sind auf einer SIM-Karte abgespeichert.

Die Zufallszahl wird in dem ausgewählten Authentifizierungsalgorithmus 24, 26, 28 eingesetzt. Jeder Authentifizierungsalgorithmus 24, 26, 28 verfügt über einen eigenen Teilnehmerschlüssel 30, 32, 34 ( $K_i$ ). Mit Hilfe des Teilnehmerschlüssels 30, 32, 34, der für jeden Authentifizierungsvorgang jedesmal erneut berechnet wird (vgl. Fig. 3), errechnet der ausgewählte Authentifizierungsalgorithmus 24, 26, 28 eine Prüfsumme 36, 38, 40. Die Prüfsumme 36, 38, 40 wird auf den Ausgang 42, 44, 46 (AUS) gegeben. Die Berechnung der Prüfsumme erfolgt bei beiden Kommunikationseinheiten, dem Mobilfunkendgerät und dem Authentifizierungszentrum (AuC) des Mobilfunknetzes, gleichzeitig. Dies kann nur dadurch erfolgen, indem bei beiden Kommunikationseinheiten die Authentifizierungsprozeduren gleichzeitig gestartet werden. Hierzu müssen neben den Adressen und Rückadressen, die miteinander ausgetauscht werden, die erforderlichen Prüfsummen (SRES, XRES), Zufallszahlen

(RAND), Teilnehmerschlüssel 30, 32, 34 ( $K_i$ ) und auch Kontrollparameter ausgetauscht werden.

In Fig. 3 wird die Erzeugung von Teilnehmerschlüsseln ( $K_i$ ) 30, 32, 34 dargestellt. Mit  $K$  wird ein Generalschlüssel bezeichnet, aus dem durch die Schlüsselgenerierungsalgorithmen ( $h_i$ ) 48, 50, 52 die digitalen Teilnehmerschlüssel hergestellt werden. Mit diesen Teilnehmerschlüsseln lassen sich jeweils die zugehörigen Authentifizierungsalgorithmen 24, 26, 28 aktivieren.

Die Authentifizierungsprozeduren erfolgen auf beiden Kommunikationseinheiten gleichzeitig. Durch die Dynamik der Auswahl des Authentifizierungsalgorithmus 30, 32, 34 und der gesonderten Berechnung der Teilnehmerschlüssel ( $K_i$ ) erhält das Authentifizierungssystem eine zusätzliche Sicherheitskomponente, ohne bei der Authentifizierung Geschwindigkeit einbüßen zu müssen. Die Authentifizierung erfolgt nämlich bei beiden Kommunikationseinheiten gleichzeitig.

### Patentansprüche

1. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten, wobei zwischen den Kommunikationseinheiten eine Authentifizierungsvereinbarung besteht, welche jeweils durch eine prozessorgestützte Authentifizierungseinheit überprüft werden kann, wobei die Authentifizierungsvereinbarung aus wenigstens zwei unterschiedlichen Authentifizierungsalgorithmen (24, 26, 28) besteht, welche in einer Speichereinheit wenigstens einer der Kommunikationseinheiten vorgesehen sind und welche durch die jeweilige andere Kommunikationseinheit zur Authentifizierung abgefragt werden kann, **dadurch gekennzeichnet, daß** Mittel zur gleichzeitigen dynamischen Verarbeitung der Authentifizierungsalgorithmen vorgesehen sind, wobei sowohl, die Adresse, als auch die entsprechende Rückadresse zwischen den Kommunikationseinheiten ausgetauscht werden.
2. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten nach Anspruch 1, **dadurch gekennzeichnet, daß** eine Kommunikationseinheit als Mobilfunkendgerät ausgebildet ist.
3. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 1 oder 2, **dadurch gekennzeichnet, daß** die Authentifizierungsalgorithmen (24, 26, 28) auf einem Teilnehmeridentitätsmodul ((U)SIM) gespeichert sind.
4. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, daß** eine Kommunikationseinheit als Authentifikationszentrale (AuC) eines Mobilfunknetzes vorgesehen ist.

5. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet, daß** wenigstens ein Authentifizierungsschlüssel (30, 32, 34) für die Authentifizierungsalgorithmen (24, 26, 28) vorgesehen ist.
6. Authentifizierungssystem bestehend aus zumindest zwei Kommunikationseinheiten nach Anspruch 5, **dadurch gekennzeichnet, daß** jedem Authentifizierungsalgorithmus (24, 26, 28) ein eigener Authentifizierungsschlüssel (30, 32, 34) zugeordnet ist.
7. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten, wobei zwischen den Kommunikationseinheiten eine Authentifizierungsvereinbarung besteht, welche jeweils durch eine prozessorgestützte Authentifizierungseinheit überprüft werden kann, wobei die Authentifizierungsvereinbarung aus wenigstens zwei unterschiedlichen Authentifizierungsalgorithmen (24, 26, 28) besteht, welche in einer Speichereinheit wenigstens einer der Kommunikationseinheiten vorgesehen sind und welche durch die jeweilige andere Kommunikationseinheit zur Authentifizierung abgefragt werden kann, **dadurch gekennzeichnet, daß** die Authentifizierungsalgorithmen (24, 26, 28) gleichzeitig dynamisch abgearbeitet werden, wobei sowohl die Adresse, als auch die entsprechende Rückadresse, zwischen den Kommunikationseinheiten ausgetauscht werden.
8. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten nach Anspruch 7, **dadurch gekennzeichnet, daß** eine Kommunikationseinheit als Mobilfunkendgerät ausgebildet ist.
9. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 7 oder 8, **dadurch gekennzeichnet, daß** die Authentifizierungsalgorithmen (24, 26, 28) auf einem Teilnehmeridentitätsmodul ((U)SIM) gespeichert werden.

10. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 7 bis 9, **dadurch gekennzeichnet, daß** eine Kommunikationseinheit als Authentifikationszentrale (AuC) eines Kommunikationsnetzes vorgesehen ist.
11. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten nach einem der Ansprüche 7 bis 10, **dadurch gekennzeichnet, daß** wenigstens ein Authentifizierungsschlüssel (30, 32, 34) für die Authentifizierungsalgorithmen (24, 26, 28) vorgesehen ist.
12. Verfahren zum Authentifizieren zwischen zumindest zwei Kommunikationseinheiten nach Anspruch 1, **dadurch gekennzeichnet, daß** jedem Authentifizierungsalgorithmus (24, 26, 28) ein eigener Authentifizierungsschlüssel (30, 32, 34) zugeordnet ist.

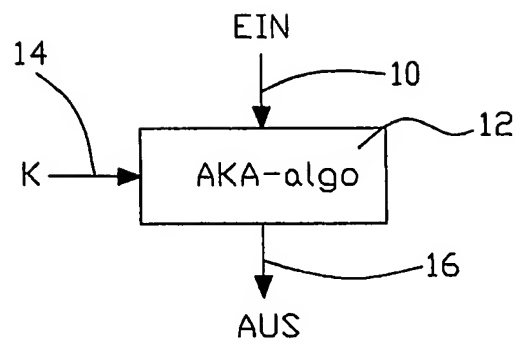


Fig.1)

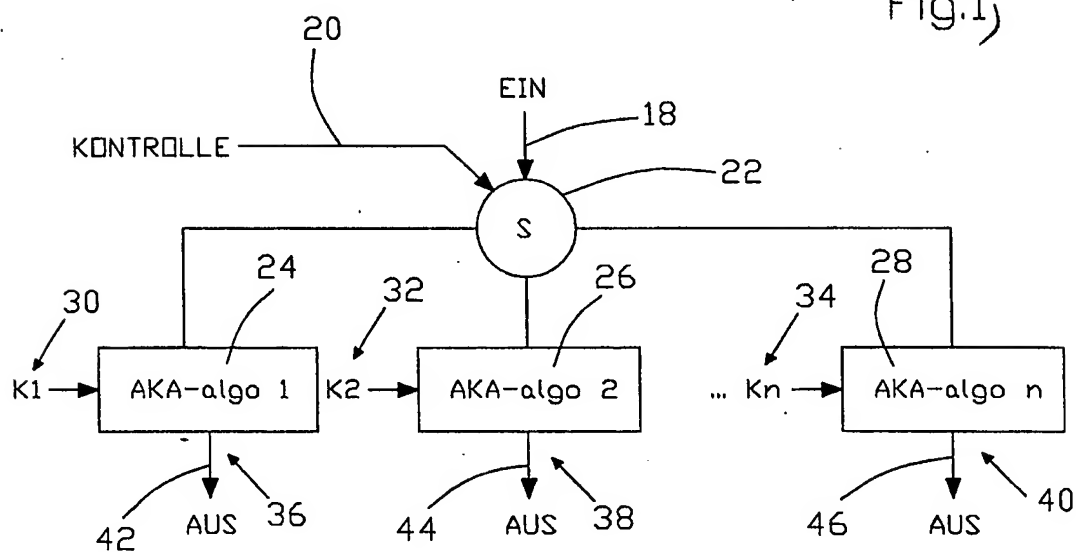


Fig.2

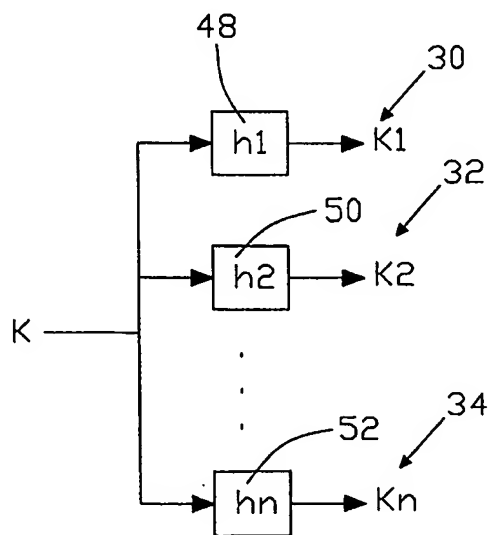


Fig.3



# PATENT COOPERATION TREATY

## PCT

### DECLARATION OF NON-ESTABLISHMENT OF INTERNATIONAL SEARCH REPORT (PCT Article 17(2)(a), Rules 13ter.1(c) and 39)

Applicant's or agent's file reference <b>WO 5014.01</b>	<b>IMPORTANT DECLARATION</b>	Date of mailing ( <i>day/month/year</i> ) <b>29/04/2003</b>
International application No. <b>PCT/EP 02/ 14411</b>	International filing date ( <i>day/month/year</i> ) <b>17/12/2002</b>	(Earliest) Priority Date ( <i>day/month/year</i> ) <b>03/01/2002</b>
International Patent Classification (IPC) or both national classification and IPC <div style="text-align: right;">H04Q7/38</div>		
Applicant <b>VODAFONE AG</b>		

This International Searching Authority hereby declares, according to Article 17(2)(a), that no international search report will be established on the international application for the reasons indicated below.

1. ☒ The subject matter of the international application relates to:
  - a. ☐ scientific theories.
  - b. ☐ mathematical theories.
  - c. ☐ plant varieties.
  - d. ☐ animal varieties.
  - e. ☐ essentially biological processes for the production of plants and animals, other than microbiological processes and the products of such processes.
  - f. ☐ schemes, rules or methods of doing business.
  - g. ☐ schemes, rules or methods of performing purely mental acts.
  - h. ☐ schemes, rules or methods of playing games.
  - i. ☐ methods for treatment of the human body by surgery or therapy.
  - j. ☐ methods for treatment of the animal body by surgery or therapy.
  - k. ☐ diagnostic methods practised on the human or animal body.
  - l. ☐ mere presentations of information.
  - m. ☐ computer programs for which this International Searching Authority is not equipped to search prior art.
  
2. ☒ The failure of the following parts of the international application to comply with prescribed requirements prevents a meaningful search from being carried out:
 

☐ the description      ☒ the claims      ☐ the drawings
  
3. ☐ The failure of the nucleotide and/or amino acid sequence listing to comply with the standard provided for in Annex C of the Administrative Instructions prevents a meaningful search from being carried out:
 

☐ the written form has not been furnished or does not comply with the standard.  
☐ the computer readable form has not been furnished or does not comply with the standard.
  
4. Further comments:

Name and mailing address of the ISA/	Authorized officer
Facsimile No.	Telephone No.

The independent Claims 1 and 7 of this international application are not defined with sufficient clarity, nor does the description contain a sufficiently clear and complete disclosure of the invention. The requirements of PCT Article 5 and 6 have therefore not been met. For these reasons it is impossible to carry out a meaningful search, and therefore, under PCT Article 17(2)(a)(ii), no international search report has been established.

The grounds for these objections are as follows:

1. Independent Claims 1 and 7 stipulate that "the authentication algorithms are dynamically executed simultaneously"; the claims thus attempt to define the subject matter in terms of the result to be attained. But this only states the problem to be solved, namely avoiding a sequential execution (see page 3, lines 25-27).

Moreover, dependent Claims 1 and 7 stipulate that "both the address and its corresponding return address are exchanged between the communications units". It is entirely unclear to what units the terms "address" and "return address" refer or how simultaneous execution of the authentication algorithms can be accomplished by said address transmission.

For the reasons indicated, independent Claims 1 and 7 do not satisfy the requirements of PCT Article 6.

2. In the description, proceeding from the GSM authentication procedure described in the prior art (page 2, lines 11-27) with its (alleged) disadvantage of sequential execution of the authentication procedures (page 3, lines 25-27), the solution proposed as per the invention is to start simultaneously and then let run in parallel the processing of the authentication algorithm (i.e. the calculation of the checksums) with the communication units taking part in the authentication procedure (page 4, lines 20-24; page 8, lines 27-31). This is accomplished, according to page 4, lines 18-20, by "simultaneously transmitting the return address along with the...address of the subscriber to be authenticated". The term "address" appears to refer to the address of the

subscriber to be authenticated. The term "return address" is not explained further in the description.

To a person skilled in the art it is not evident what connection there is between the transmission of an address of a subscriber and of an undefined retrun address and the simultaneous execution of an authentication procedure in two communications units, or how a parallel starting of the authentication procedures can be accomplished by this address transmission.

Proceeding from the indicated prior art it is also unclear what is meant by the terms "address" and "return address", since these terms are not used there.

Nor does the second mention of "address" and "return address" in the description on page 8, line 31 to page 9, line 2 give a person skilled in the art any help in putting the invention into practice, since there too no explanation is given as to what "return address" refers to or what effect at all the transmission of addresses has.

For these reasons the description in this international application does not satisfy the requirements specified in PCT Article 5 and in the PCT Guidelines, Chapter II, 4.1.

The applicant is advised that claims relating to inventions in respect of which no international search report has been established normally cannot be the subject of an international preliminary examination (PCT Rule 66.1(e)). In its capacity as International Preliminary Examining Authority the EPO generally will not carry out a preliminary examination for subjects that have not been searched. This also applies to cases where the claims were amended after receipt of the international search report (PCT Article 19) or where the applicant submits new claims in the course of the procedure under PCT Chapter II. After entry into the regional phase before the EPO, however, an additional search can be carried out in the course of the examination (cf. EPO Guidelines, Part C, VI, 8.5) if the deficiencies that led to the declaration under PCT Article 17(2) have been remedied.

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### ERKLÄRUNG ÜBER DIE NICHTERSTELLUNG EINES INTERNATIONALEN RECHERCHENBERICHTS

(Artikel 17 (2) a) und Regeln 13ter. 1 c) und 39 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>WO 5014.01</b>	<b>WICHTIGE ERKLÄRUNG</b>	Absenddatum (Tag/Monat/Jahr) <b>29/04/2003</b>
Internationales Aktenzeichen <b>PCT/EP 02/14411</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>17/12/2002</b>	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>03/01/2002</b>
Internationale Patentklassifikation (IPC) oder nationale Klassifikation und IPC <div style="text-align: right;">H04Q7/38</div>		
Anmelder <b>VODAFONE AG</b>		

Die Internationale Recherchenbehörde erklärt gemäß Artikel 17(2)a), daß für die internationale Anmeldung aus den nachstehend aufgeführten Gründen kein internationaler Recherchenbericht erstellt wird.

1. ☒ Der Gegenstand der internationalen Anmeldung betrifft folgende Gebiete:
  - a. ☐ wissenschaftliche Theorien.
  - b. ☐ mathematische Theorien.
  - c. ☐ Pflanzensorten.
  - d. ☐ Tierarten.
  - e. ☐ im wesentlichen biologische Verfahren zur Züchtung von Pflanzen und Tieren mit Ausnahme mikrobiologischer Verfahren und der mit Hilfe dieser Verfahren gewonnenen Erzeugnisse.
  - f. ☐ Pläne, Regeln und Verfahren für eine geschäftliche Tätigkeit.
  - g. ☐ Pläne, Regeln und Verfahren für rein gedankliche Tätigkeiten.
  - h. ☐ Pläne, Regeln und Verfahren für Spiele.
  - i. ☐ Verfahren zur chirurgischen oder therapeutischen Behandlung des menschlichen Körpers.
  - j. ☐ Verfahren zur chirurgischen oder therapeutischen Behandlung des tierischen Körpers.
  - k. ☐ Diagnostizierverfahren zur Anwendung am menschlichen oder tierischen Körper.
  - l. ☐ bloße Wiedergabe von Informationen.
  - m. ☐ Programme von Datenverarbeitungsanlagen, in bezug auf die die Internationale Recherchenbehörde nicht für die Durchführung einer Recherche über den Stand der Technik ausgerüstet ist.
2. ☒ Die folgenden Teile der internationalen Anmeldung entsprechen nicht den vorgeschriebenen Anforderungen so daß eine sinnvolle Recherche nicht durchgeführt werden kann:
 

☐ die Beschreibung
☒ die Ansprüche
☐ die Zeichnungen
3. ☐ Das Protokoll der Nucleotid- und/oder Aminosäuresequenzen entspricht nicht dem in Anlage C der Verwaltungsvorschriften vorgeschriebenen Standard, so daß eine sinnvolle Recherche nicht durchgeführt werden kann.
 

☐ Die schriftliche Form wurde nicht eingereicht bzw. entspricht nicht dem Standard.

☐ Die computerlesbare Form wurde nicht eingereicht bzw. entspricht nicht dem Standard.
4. Weitere Bemerkungen: See additional sheets.

Name und Postanschrift der Internationalen Recherchenbehörde  

 Europäisches Patentamt, P.B. 5818 Patentlaan 2  
 NL-2280 HV Rijswijk  
 Tel. (+31-70) 340-2040  
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Patricia Sánchez Gómez

## WEITERE ANGABEN

PCT/ISA/ 203

Die unabhängigen Ansprüche 1 und 7 dieser Internationalen Anmeldung sind nicht ausreichend klar und deutlich definiert und auch die Beschreibung enthält keine ausreichend deutliche und vollständige Offenbarung der Erfindung. Die Erfordernisse der Artikel 5 und 6 PCT sind daher nicht erfüllt. Da eine aussagefähige und sinnvolle Recherche aus diesen Gründen nicht möglich ist, wird gemäß Artikel 17(2)(a) (ii) PCT kein Internationaler Recherchenbericht erstellt.

Die Einwände werden folgendermaßen begründet:

1. Die unabhängigen Ansprüche 1 und 7 definieren, dass "die Authentifizierungsalgorithmen gleichzeitig dynamisch abgearbeitet werden"; es wird also versucht, den Gegenstand durch das zu erreichende Ergebnis zu definieren. Damit wird aber lediglich die zu lösende Aufgabe angegeben, nämlich die Vermeidung einer sequentiellen Abarbeitung (siehe Seite 3, Zeilen 25-27).

Darüber hinaus definieren die unabhängigen Ansprüche 1 und 7, dass "sowohl die Adresse als auch die entsprechende Rückadresse zwischen den Kommunikationseinheiten ausgetauscht wird". Es ist völlig unklar, auf welche Einheiten sich die Begriffe "Adresse" bzw. "Rückadresse" beziehen, sowie warum durch die genannte Adressübertragung eine gleichzeitige Abarbeitung der Authentifizierungsalgorithmen erreicht werden kann.

Die unabhängigen Ansprüche 1 und 7 genügen aus den genannten Gründen nicht den Erfordernissen des Artikels 6 PCT.

2. In der Beschreibung wird diesbezüglich ausgehend von der als Stand der Technik beschriebenen GSM-Authentifizierungsprozedur (Seite 2, Zeilen 11-27) mit dem (angeblichen) Nachteil des sequentiellen Abarbeitens der Authentifizierungsvorgänge (Seite 3, Zeilen 25-27) als erfindungsgemäße Lösung vorgeschlagen, die Verarbeitung des Authentifizierungsalgorithmus (d.h. die Berechnung der Prüfsummen) bei den an einem Authentifizierungsvorgang beteiligten Kommunikationseinheiten gleichzeitig zu starten und dann parallel ablaufen zu lassen (Seite 4, Zeilen 20-24; Seite 8, Zeilen 27-31). Dies wird gemäß Seite 4, Zeilen 18-20 dadurch erreicht, daß "neben der ... Adresse des Teilnehmers der authentifiziert werden soll, gleichzeitig die Rückadresse übermittelt wird". Der Begriff "Adresse" scheint sich auf die Adresse des zu authentifizierenden Teilnehmers zu beziehen. Der Begriff "Rückadresse" wird in der Beschreibung nicht weiter erläutert.

Es ist für den Fachmann nicht erkennbar, welcher Zusammenhang zwischen der Übertragung einer Adresse eines Teilnehmers sowie einer nicht weiter definierten Rückadresse und der gleichzeitigen Abarbeitung einer Authentifizierungsprozedur in zwei Kommunikationseinheiten besteht, bzw. warum durch diese Adressübertragung ein paralleles Starten der Authentifizierungsprozeduren erreicht werden kann.

Ausgehend vom dargestellten Stand der Technik ist ebenfalls nicht erkennbar, wie die Begriffe "Adresse" und "Rückadresse" zu verstehen sind, da diese Begriffe dort nicht verwendet werden.

Auch das zweite Auftreten der Begriffe "Adresse" und "Rückadresse" in der Beschreibung auf Seite 8, Zeile 31 - Seite 9, Zeile 2 gibt dem Fachmann

## WEITERE ANGABEN

PCT/ISA/ 203

keinerlei Hilfestellung zur Umsetzung der Erfindung in die Praxis, da auch dort nicht erläutert wird, worauf sich die "Rückadresse" bezieht und welchen Effekt die Übertragung von Adressen überhaupt hat.

Die Beschreibung dieser Internationalen Anmeldung genügt aus den genannten Gründen nicht den in Artikel 5 PCT sowie in den PCT-Richtlinien, Kapitel II, 4.1, genannten Erfordernissen.

Der Anmelder wird darauf hingewiesen, daß Patentansprüche auf Erfindungen, für die kein internationaler Recherchenbericht erstellt wurde, normalerweise nicht Gegenstand einer internationalen vorläufigen Prüfung sein können (Regel 66.1(e) PCT). In seiner Eigenschaft als mit, der internationalen vorläufigen Prüfung beauftragte Behörde wird das EPA also in der Regel keine vorläufige Prüfung für Gegenstände durchführen, zu denen keine Recherche vorliegt. Dies gilt auch für den Fall, daß die Patentansprüche nach Erhalt des internationalen Recherchenberichtes geändert wurden (Art. 19 PCT), oder für den Fall, daß der Anmelder im Zuge des Verfahrens gemäß Kapitel II PCT neue Patentansprüche vorlegt. Nach Eintritt in die regionale Phase vor dem EPA kann jedoch im Zuge der Prüfung eine weitere Recherche durchgeführt werden (Vgl. EPA-Richtlinien C-VI, 8.5), sollten die Mängel behoben sein, die zu der Erklärung gemäß Art. 17 (2) PCT geführt haben.